International Journal of Advanced Multidisciplinary Research and Educational Development
2026 | www.ijamred.com
ISSN: 3107-6513

ADRecon-X: Active Directory Reconnaissance Tool

Hari Krishnan A
Guided By:Dr.T.Velumani
Department of Computer Science, Rathinam College of Arts and Science (Autonomous), Coimbatore, Tamil Nadu, India.

Abstract*—Active Directory (AD) is the backbone of identity and access management in enterprise environments, managing users, groups, computers, and access control policies across organizational networks. Due to its centralized authority, Active Directory has become a primary target for cyberattackers seeking unauthorized access, privilege escalation, and lateral movement. Traditional reconnaissance methods for assessing Active Directory security rely on fragmented manual tools, command-line utilities, and Windows-dependent processes that are time-consuming, inconsistent, and difficult for beginners to interpret. This paper presents ADRecon-X, a Linux-based Active Directory reconnaissance framework designed to automate the discovery, enumeration, and analysis of enterprise Active Directory environments. The system integrates multiple reconnaissance modules including network discovery, domain user enumeration, group membership analysis, privilege identification, and risk scoring into a single centralized workflow. By operating entirely from a Linux platform using standard LDAP protocols, ADRecon-X eliminates dependency on domain-joined Windows machines and improves operational flexibility. The framework generates structured, readable outputs in the form of tables, logs, and risk assessment summaries that help security professionals, students, and administrators understand domain structures and identify potential security weaknesses. Experimental evaluation in a controlled virtual Active Directory environment demonstrates that ADRecon-X effectively performs comprehensive reconnaissance with minimal manual effort, reduced human error, and improved assessment consistency compared to traditional fragmented approaches.*

Keywords*—Active Directory, Reconnaissance, Cybersecurity, Privilege Escalation, Domain Enumeration, Endpoint Security, Linux, Digital Forensics, Kerberoasting, LDAP.*

I. INTRODUCTION

The increasing reliance of enterprises on centralized directory services has made Active Directory one of the most critical and widely targeted components in organizational cybersecurity. Active Directory manages authentication, authorization, users, groups, computers, and access control policies across enterprise networks. Due to its centralized control over critical resources and its widespread deployment across corporate infrastructures globally, Active Directory has become a high-value target for security breaches caused by misconfigurations, excessive privileges, and weak access controls. As organizations scale their IT environments, the complexity of Active Directory grows, making regular security assessment and continuous visibility into domain structures a fundamental requirement rather than an optional practice.

Although significant progress has been made in developing security assessment tools, many existing reconnaissance solutions rely on manual techniques, independent command-line utilities, and multiple fragmented tools that operate in isolation. These approaches are time-consuming, prone to human error, and difficult for beginners or students to interpret meaningfully. Furthermore, most traditional reconnaissance tools are designed for Windows-based environments and require domain-joined machines or elevated administrative access, which limits their flexibility and practical applicability in modern cybersecurity assessment contexts that increasingly prefer Linux-based platforms.

Several researchers have proposed different approaches to Active Directory security analysis. Some methods focus on manual enumeration using tools such as net user, nltest, and PowerView in Windows environments. Others use BloodHound for graphical relationship mapping, though this requires installation of agents and database components. Command-line tools like ldapsearch provide raw enumeration capabilities but require significant expertise to interpret outputs meaningfully. Despite these existing efforts, challenges such as fragmented workflow, platform dependency, and lack of structured output for beginners continue to limit the practical usability of these approaches.

There is therefore a clear need for a centralized, automated, and beginner-friendly Active Directory reconnaissance framework that can operate from a Linux environment, integrate multiple reconnaissance techniques into a single workflow, and present findings in structured and interpretable formats. This paper introduces ADRecon-X, a Linux-based Active Directory reconnaissance tool that addresses these limitations and provides a practical solution for ethical cybersecurity assessment and education. The proposed system focuses on automating domain enumeration, privilege analysis, and risk scoring to improve the efficiency and accuracy of Active Directory security assessments.

II. RELATED WORKS

Several approaches have been proposed for Active Directory reconnaissance and security analysis using different cybersecurity techniques and tools. Early methods relied on native Windows administrative commands such as net user, net group, and nltest to manually gather domain information, but these approaches require significant technical expertise and produce unstructured outputs that are difficult to correlate and analyze efficiently.

BloodHound, a widely used tool for Active Directory attack path analysis, introduced graph-based visualization of domain relationships and privilege paths. However, BloodHound requires the deployment of SharpHound collectors on Windows machines and a Neo4j database backend, which limits its applicability in lightweight Linux-based assessment scenarios. Similarly, tools like PowerSploit and PowerView provide extensive Active Directory enumeration capabilities but depend on Windows PowerShell environments, restricting their use in cross-platform security assessments.

LDAP-based enumeration approaches using tools such as ldapsearch and impacket libraries have demonstrated the feasibility of performing Active Directory reconnaissance from Linux environments without requiring domain-joined machines. These

approaches use standard LDAP protocols to query directory services and collect user, group, and policy information. Impacket-based tools like GetUserSPNs have specifically addressed Kerberoasting attack identification, which targets service account vulnerabilities in Active Directory environments.

Despite these advancements, existing methods still face challenges such as fragmented workflows requiring multiple tools, lack of unified risk scoring, poor structured output for beginners, and absence of an integrated single-tool solution that covers the full Active Directory reconnaissance lifecycle from network discovery through privilege analysis to reporting. These limitations highlight the need for a centralized, automated, and educational framework that simplifies the full Active Directory reconnaissance process while maintaining ethical usage boundaries.

III. SYSTEM DESIGN

The background research highlights a clear need for an automated and centralized Active Directory reconnaissance framework that operates from a Linux environment and provides structured, interpretable security assessment outputs. This study introduces ADRecon-X, an optimized framework for identifying Active Directory vulnerabilities by analyzing domain structures, user privileges, group memberships, and configuration weaknesses. The primary contributions of this study are as follows:

- Implementing automated domain enumeration to collect user accounts, group memberships, and organizational unit information without manual command execution.
- Integrating multiple reconnaissance modules into a single centralized workflow operating from a Linux platform using standard LDAP and authentication protocols.
- Applying a risk scoring mechanism to evaluate domain security posture and identify privilege escalation paths, Kerberoastable service accounts, and misconfigured access controls.
- Generating structured, readable outputs in the form of tables, logs, and summary reports suitable for security professionals, students, and academic evaluation.

3.1. Network Discovery and Input Validation

The process begins with the user providing required parameters through the command-line interface, including the domain controller IP address, domain name, and authorized credentials. The Input Validation Module verifies that all inputs are correctly formatted and that the domain controller is reachable on the network before initiating any reconnaissance operations. This validation step prevents incorrect execution, ensures connectivity with the Active Directory environment, and maintains system stability during subsequent enumeration phases.

3.2. Domain User and Group Enumeration

The User Enumeration Module connects to the Active Directory domain using standard LDAP protocols and collects information about all domain user accounts, including usernames, account status, and privilege attributes. The Group Enumeration Module subsequently identifies Active Directory groups and their associated members. Since permissions and access rights in Active Directory are commonly assigned through group memberships, this module plays a critical role in revealing access control structures, identifying over-privileged accounts, and detecting groups with elevated administrative access such as Domain Admins, Enterprise Admins, and Schema Admins.

3.3. Privilege Analysis and Risk Scoring

The Privilege Analysis Module examines the permissions and access rights associated with enumerated users and groups to identify accounts with administrative or elevated access. This module specifically identifies Kerberoastable service accounts, whose service tickets can be targeted for offline password attacks, and checks for the presence of AS-REP Roastable accounts that do not require Kerberos preauthentication. A risk scoring mechanism aggregates findings across all enumerated data points and assigns an overall risk score on a scale of 0 to 100, along with a corresponding risk level classification (Low, Medium, or High), enabling users to prioritize remediation actions effectively.

3.4. Reporting and Structured Output

The Reporting Module consolidates all reconnaissance findings and generates structured outputs in tabular and summary report formats. The outputs include domain user listings, group membership tables, privileged account summaries, Kerberoastable account warnings, and the overall risk assessment result. All output files are stored locally on the assessment machine, ensuring data privacy and user control. The structured presentation minimizes complexity for beginners and allows security professionals to quickly understand domain structure and security posture without additional post-processing.

IV. OBJECTIVE AND SCOPE

The primary objective of this research is to develop ADRecon-X, a centralized and automated Linux-based Active Directory reconnaissance framework that simplifies the assessment of enterprise directory service environments. The system aims to accurately enumerate domain users, groups, and privileges, identify Kerberoastable service accounts and over-privileged access paths, evaluate the overall domain security posture, and present findings in structured and interpretable formats suitable for both beginners and experienced security professionals. This study further seeks to demonstrate that automating the Active Directory reconnaissance lifecycle reduces manual effort, minimizes human error, and improves assessment consistency compared to existing fragmented approaches.

The scope of this research includes the design, development, and evaluation of the ADRecon-X framework in controlled virtual Active Directory laboratory environments. The system covers network discovery, domain user and group enumeration, privilege analysis, Kerberoasting vulnerability identification, and risk score generation. ADRecon-X is designed exclusively for ethical usage in authorized environments and does not perform exploitation, credential cracking, or any intrusive or destructive actions against Active Directory infrastructure. The framework is suitable for academic projects, cybersecurity training programs, penetration testing laboratories, and authorized enterprise security assessments.

V. LITERATURE REVIEW

Active Directory security assessment and reconnaissance have gained significant attention in cybersecurity research due to the increasing frequency of identity-based attacks targeting enterprise directory services. The centralized nature of Active Directory, combined with its widespread deployment across corporate infrastructures, makes it a critical component requiring continuous security monitoring and assessment. A review of existing literature highlights both the advances in Active Directory security tools and the limitations that continue to affect their practical usability in real-world and educational environments.

Early research on Active Directory security focused primarily on manual enumeration techniques using native Windows administrative tools. These approaches, while functional, required deep technical knowledge and produced unstructured outputs that were difficult to correlate across large enterprise environments. Subsequent research introduced automated tools such as BloodHound, which revolutionized Active Directory attack path analysis through graph-based visualization. However, BloodHound relies on the deployment of Windows-based collection agents and a Neo4j graph database, creating operational complexity that limits its use in lightweight assessment scenarios.

Kerberoasting, first documented by Medin in 2014 and expanded upon by Metcalf, demonstrated that service account vulnerabilities in Active Directory could be exploited to perform offline password attacks against Kerberos service tickets. This research prompted the development of targeted enumeration tools such as impacket's GetUserSPNs, which identify Kerberoastable accounts from Linux environments. Similarly, the AS-REP Roasting technique identified accounts not requiring Kerberos preauthentication as an additional attack vector. These specialized tools, however, address only specific vulnerability types rather than providing holistic Active Directory assessment capabilities.

Research by Bx and colleagues emphasized the need for centralized and unified Active Directory security assessment frameworks that integrate multiple reconnaissance techniques, reduce operational complexity, and support cross-platform execution. Their findings highlighted that fragmented tool ecosystems increase the risk of missed findings and make consistent assessment reporting difficult. This aligns with the motivation for ADRecon-X, which addresses the gap between specialized individual tools and a comprehensive, beginner-friendly, Linux-based reconnaissance framework suitable for both educational and professional cybersecurity environments.

VI. OUTPUT

ADRecon-X generates structured, command-line-formatted outputs upon completing the reconnaissance workflow. The output begins with Active Directory root discovery, presenting the Forest Root Naming Context and Domain Naming Context. It then displays a formatted table of all discovered domain users, followed by a comprehensive list of domain groups including privileged groups such as Domain Admins, Enterprise Admins, and Schema Admins. Privileged groups are highlighted with warning indicators to draw immediate attention to high-risk accounts. Kerberoastable service accounts are separately identified and flagged with risk annotations explaining the potential for offline password attacks. The final output section presents the Risk Assessment Summary, including the overall risk score and risk level classification, along with a concise list of key findings identified during the assessment.

A sample output of ADRecon-X on a test Active Directory environment produced the following summarized results: Forest Root Naming Context: DC=corp,DC=local; Domain users discovered including Administrator, Guest, DC01$, and testuser; Domain groups enumerated including Administrators, Domain Admins, Enterprise Admins, Schema Admins, Domain Users, Remote Desktop Users, Backup Operators, Server Operators, and Account Operators; Privileged groups identified: Administrators, Domain Admins, Enterprise Admins, Schema Admins; No AS-REP Roastable accounts found; Kerberoastable service accounts found including DC01$ and krbtgt with risk annotation; Overall Risk Score: 60/100 at MEDIUM level.

VII. RESULTS

The results obtained from ADRecon-X are presented in a structured format to evaluate its effectiveness in performing Active Directory reconnaissance and security assessment. The performance is analyzed based on the completeness of domain enumeration, accuracy of privilege identification, detection of Kerberoastable service accounts, and quality of the risk assessment summary. The results are organized by reconnaissance module to clearly highlight the contribution of each component to the overall assessment workflow.

TABLE I. ADRecon-X Reconnaissance Module Results

Module / Technique	Description	Observation
Network Discovery	Verifies domain controller connectivity and AD service availability	Domain controller located; AD services confirmed active
User Enumeration	Collects domain user accounts, usernames, and account attributes	All domain users enumerated with account status identified
Group Enumeration	Identifies AD groups, membership structures, and access policies	Privileged groups (Domain Admins, Enterprise Admins) and members listed
Privilege Analysis	Detects accounts with administrative or elevated access rights	Kerberoastable service accounts and over-privileged users detected
Risk Assessment	Evaluates overall domain security posture and assigns risk score	Risk Score: 60/100 — Level: MEDIUM; actionable findings generated

The system performance remained stable across all reconnaissance modules without significant resource overhead. The Network Discovery and User Enumeration modules completed within seconds on the test environment, while the Privilege Analysis module

accurately identified Kerberoastable service accounts and over-privileged group memberships. The Risk Assessment module correctly computed a score of 60 out of 100 and classified the domain security posture as MEDIUM risk, reflecting the presence of privileged groups and service account exposure without AS-REP roasting vulnerabilities.

The results confirm that ADRecon-X successfully performs comprehensive Active Directory reconnaissance in a centralized, automated, and Linux-based workflow. The structured output format significantly reduces the effort required to interpret domain findings compared to raw command-line tool outputs. The framework accurately identifies both basic domain structure information and critical security misconfigurations, enabling users to prioritize remediation actions based on the severity of identified risks. Compared to manual approaches using multiple independent tools, ADRecon-X reduces assessment time and minimizes the likelihood of missed findings due to incomplete manual correlation.

Recent studies have emphasized the importance of automated and structured approaches for Active Directory security assessments in enterprise environments. By integrating domain user enumeration, group analysis, privilege identification, and Kerberoasting vulnerability detection into a single workflow, ADRecon-X demonstrates improved efficiency, consistency, and usability compared to existing fragmented reconnaissance methods. The framework shows particular strength in educational and training contexts, where structured and readable outputs help learners understand complex domain relationships without requiring prior expertise in Active Directory internals.

VIII. CONCLUSION

The proposed ADRecon-X framework for Active Directory reconnaissance using automated Linux-based techniques provides effective, reliable, and structured results in assessing enterprise domain security posture. By analyzing domain configurations, user privilege structures, group memberships, and Kerberoasting vulnerabilities through a centralized and automated workflow, the system accurately distinguishes security weaknesses and presents actionable findings in an organized format. Among the techniques employed, privilege analysis and Kerberoastable account detection proved particularly effective in identifying high-risk attack surfaces within the test Active Directory environment.

By incorporating domain user enumeration, group membership analysis, organizational unit mapping, and real-time risk scoring, ADRecon-X identifies complex domain security patterns and supports better decision-making in securing enterprise Active Directory environments. Although challenges such as evolving attack techniques, domain-specific configurations, and cloud Active Directory environments exist, continuous improvements through integration of machine learning-based anomaly detection and support for Azure AD reconnaissance can further enhance the framework's capabilities. Overall, the proposed approach provides a scalable, ethical, and efficient solution for Active Directory security assessment and contributes meaningfully to strengthening modern cybersecurity education and practice.

ACKNOWLEDGMENT

This article is the outcome of the research work carried out in the Department of Computer Science, Rathinam College of Arts and Science (Autonomous), Coimbatore. The author would like to express sincere gratitude to Dr. T. Velumani, Head of the Department of Computer Science, for his valuable guidance, constructive suggestions, and continuous encouragement throughout the development of this work. We also extend sincere thanks to Sprout Knowledge Solutions Pvt. Ltd., Coimbatore, for providing the organizational environment and resources to undertake and complete this project from December 2025 to April 2026. The support of all faculty members and mentors in the department has greatly contributed to the successful completion of this research.

REFERENCES

[1] Microsoft Corporation, "Active Directory Domain Services Overview," Microsoft Docs, 2022. [Online]. Available: https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/

[2] Metcalf, S., "Kerberoasting: Attacking Kerberos Service Accounts," Active Directory Security Blog, 2014.

[3] NIST, "Framework for Improving Critical Infrastructure Cybersecurity," National Institute of Standards and Technology, 2018.

[4] Center for Internet Security (CIS), "CIS Critical Security Controls," Version 8, 2021.

[5] OWASP Foundation, "OWASP Top 10: The Ten Most Critical Web Application Security Risks," 2021.

[6] W. Stallings, Network Security Essentials: Applications and Standards, 6th ed., Pearson, 2018.

[7] M. Bishop, Computer Security: Art and Science, Addison-Wesley, 2003.

[8] Forshaw, J., Attacking Network Protocols: A Hacker's Guide to Capture, Analysis, and Exploitation, No Starch Press, 2018.

[9] Graeber, M., "Abusing Active Directory Permissions with PowerView," DEF CON 25, 2017.

[10] Robbins, A., Blundell, R., and Vazarkar, R., "BloodHound: Six Degrees of Domain Admin," DEF CON 24, 2016.